CLAIMS

1. A method of allocating an address to a certificate to be stored in an addressable database for subsequent retrieval, said method comprising the steps of generating a string for use as a certificate locator from information contained in a certificate request and utilizing said string to obtain said address.

2. A method according to claim 1 wherein said string is mapped to an address in said directory.

3. A method according to claim 1 wherein said string is used as said address in said directory.

4. A method according to claim 1 wherein a mathematical function is applied to said information to obtain said string.

5. A method according to claim 4 wherein said mathematical function is a hash function.

6. A method according to claim 5 wherein said string is a portion of the output of said hash function.

7. A method of identifying an address of a certificate to a recipient of a signed message in a data communication system, said method comprising the steps of preparing a set of information for inclusion in a certificate request, generating from said set of information a string for use as a certificate locator in a database, and forwarding said string to said recipient to indicate the location of said certificate in said database.

8. A method according to claim 7 wherein said information includes a time varying element.

9. A method according to claim 7 wherein a predetermined mathematical function is applied to said information to obtain said string.

10. A method for maintaining certificates in a public key infrastructure having a certification authority and a pair of correspondents, said method comprising the steps of collating at one of said correspondents information comprising a request for a certificate of said certification authority, forwarding said request to said certification authority, computing from said information comprising said request a string for use as a certificate locator by said one correspondent and said certification authority, storing a certificate issued from said request in a directory at an address obtained from said

12

1   string and forwarding said locator from said one correspondent to another permit

2   retrieval of said certificate from said directory.

3   11. A method according to claim 10 wherein said information includes a time varying

4   element.

5   12. A method according to claim 10 wherein communication between said one

6   correspondent and said certification authority is performed over a secure channel.

7   13. A method according to claim 10 wherein said other correspondent obtains an address

8   of said certificate from a known address of said directory and said string.

9   14. A method according to claim 10 wherein said other correspondent forwards said

10   locator to said certification authority for construction of said address.

11   15. A method according to claim 10 wherein said string is computed by application of a

12   cryptographic hash function at least part of said request.

13   16. A method according to claim 15 wherein said part includes a time varying element.

14   17. A method according to claim 15 wherein a portion of the output of said hash function

15   is used as said bit string.

16   18. A method according to claim 10 wherein said but string is utilised as a pointer to an

17   address in a directory.